Resilience^{N} – a Multi-Dimensional Challenge for Maritime Infrastructures

Otpornost – višedimenzionalni izazov za pomorsku infrastrukturu

Evelin Engler
German Aerospace Center (DLR)
Institute of Communication and Navigation
e-mail: Evelin.Engler@dlr.de

Dennis Göge
German Aerospace Center (DLR)
Institute for the Protection of Maritime Infrastructures
e-mail: pks22839@dlr.de

Stephan Brusch
German Aerospace Center (DLR)
Programme Coordination
Defence & Security Research
e-mail: Stephan.Brusch@dlr.de

DOI 10.17818/NM/2018/2.8
UDK 627.76/77:656.61
Review / *Pregledni rad*
Paper accepted / *Rukopis primljen:* 14. 1. 2018.

Summary

One of the definitions describes resilience as the "ability of a system, community or society to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner" [6]. The increasing demand for resilience arises from a steadily growing culture of safety as well as emerging threats. Maritime infrastructures are also affected by this. This article discusses the relationship between resilience, safety and safety objectives using case examples from the maritime domain. Principal approaches for the increase of resilience are described and typical indicators used to specify and evaluate the performance, to identify risks and to initiate compensation measures are explained. A generic process model is proposed to achieve a comprehensive, N-dimensional, view on proactive and reactive aspects of resilience engineering in relation to the entity's lifecycle and to external factors such as needs, monitors and control mechanisms.

KEY WORDS
resilience
safety and safety objectives
security
key threats and identifiers

Sažetak

Jedna od definicija opisuje otpornost kao "sposobnost sustava, zajednice ili društva da se odupre, apsorbira, prilagodi i oporavi od učinaka opasnosti na pravodoban i učinkovit način" [6]. Povećana potreba za otpornošću rezultat je stalno rastuće kulture sigurnosti, kao i nadolazećih prijetnji. To utječe i na pomorske infrastrukture. U članku se problematizira odnos između otpornosti, sigurnosti i ciljeva sigurnosti na primjerima iz pomorstva. Opisani su glavni pristupi povećanju otpornosti, a objašnjeni su tipični pokazatelji kojima se koristi za određivanje i procjenu učinka, identificiranje rizika i pokretanje kompenzacijskih mjera. Predložen je generički model procesa kako bi se postigao sveobuhvatni N-dimenzionalni pogled na proaktivne i reaktivne aspekte inženjerstva otpornosti u odnosu prema životnom ciklusu subjekta i na vanjske čimbenike, poput potreba, nadzora i kontrolnih mehanizama.

KLJUČNE RIJEČI
otpornost
ciljevi sigurnosti i zaštite
sigurnost
glavne prijetnje i pokazatelji

1. BACKGROUND / *Kontekst*

The definition and understanding of what resilience entails is dependent on the professional area and technical jargon in which the objectives are pursued – either on a technical, economical, ecological or social level. The United Nations Office for Disaster Risk Reduction defined resilience as "the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions" [6]. The European Commission considers resilience as the "ability of an individual, a household, a community, a country or a region to withstand, to adapt, and to quickly recover from stresses and shocks" [2].

What these and other definitions have in common is that the term resilience is used to formulate two complementary requirements: The first requirement focuses on the intended resistance of the entity[1] to normal conditions. Assuming that the design and realisation of the entity is in compliance with the specifications, it may be expected that, under normal conditions, the entity is able to perform the specified functionality (in operation) and to fulfil the performance requirements (Fig. 1). In the case of slightly different conditions, e.g. moderate external disturbances, more intense traffic, bad weather, or failures of single components, the functionality of the entity should be ensured with a tolerable reduction in performance. Highly degraded conditions as well as increased threats lead to an intolerable loss of performance, break down of functionality, or in the worst case to the destruction of the entity. The second requirement asks for the ability of the entity or superordinate system to reduce the adverse impact of such events.

[1] *Entity is used in the paper as a generalisation for system of systems, services, community, society, individual, household, country or region.*

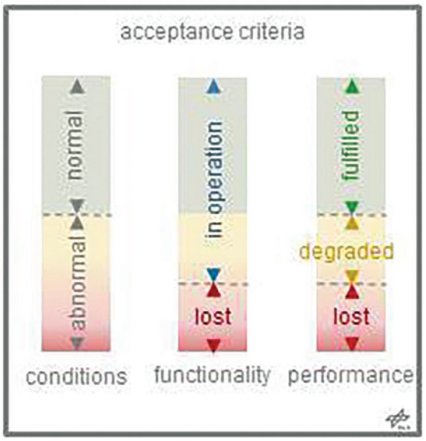

Figure 1 Acceptance criteria for design and operation
Slika 1. Kriteriji prihvatljivosti za projektiranje i rad

Figure2 illustrates complementary ways to increase the resilience of an entity. The graph (2.0) shows the typical behaviour of an entity: during nominal conditions it fulfils its functionality (green), and during abnormal conditions the functionality is degraded (yellow) or lost (red). From time to time the entity is maintained to keep the functionality on par with the supported resistance level. The graph (2.a) shows the behaviour of the entity that was improved during maintenance and thus has a decreased vulnerability. This case excludes that the entity becomes more sensitive to other or new threats by modernisation. Representative examples are the use of interference and multipath mitigation techniques to increase the performance of positioning based on Global Navigation Satellite Systems (GNSS) or the implementation of patches to protect computers against cyber-attacks. The second method is illustrated by the graph (2.b). It should be noted that a 100 percent working entity is unrealistic because any entity may support only a certain level of resilience in relation to the known and unknown threats. The design of a system that can withstand cascade effects is particularly difficult. One common approach to compensate breakdowns of any kind is to equip the entity with a backup, which means installing a second functional component that is able to perform the same task independently from the first, possibly with lower performance. For instance, the carriage requirement of a ship to have additional and preferably independent navigation sensors is an appropriate measure to avoid single sensor failures leading to insufficient situational awareness. The graph (2.c) illustrates that resilience may also be improved by implementing effective damage containment, thus reducing social, ecological or economical harms and/or facilitating a fast recovery of the entity after the occurrence of disruptive events. A typical example is the provision of emergency services to repair and/or recover ships where possible.

Resilience Engineering sees itself "as a new way of thinking about safety" [4] and establishes also new opportunities for the maritime domain [8]. This implies that the objective of resilience engineering is maintaining safety. Growing threats of terrorism, piracy and crime make it impossible to consider safety and security aspects as independent factors. This is quite understandable, if we consider the increasing importance of cybersecurity for the safety of society and the economy (e.g. transport, energy, medical supply). Increasing complexity

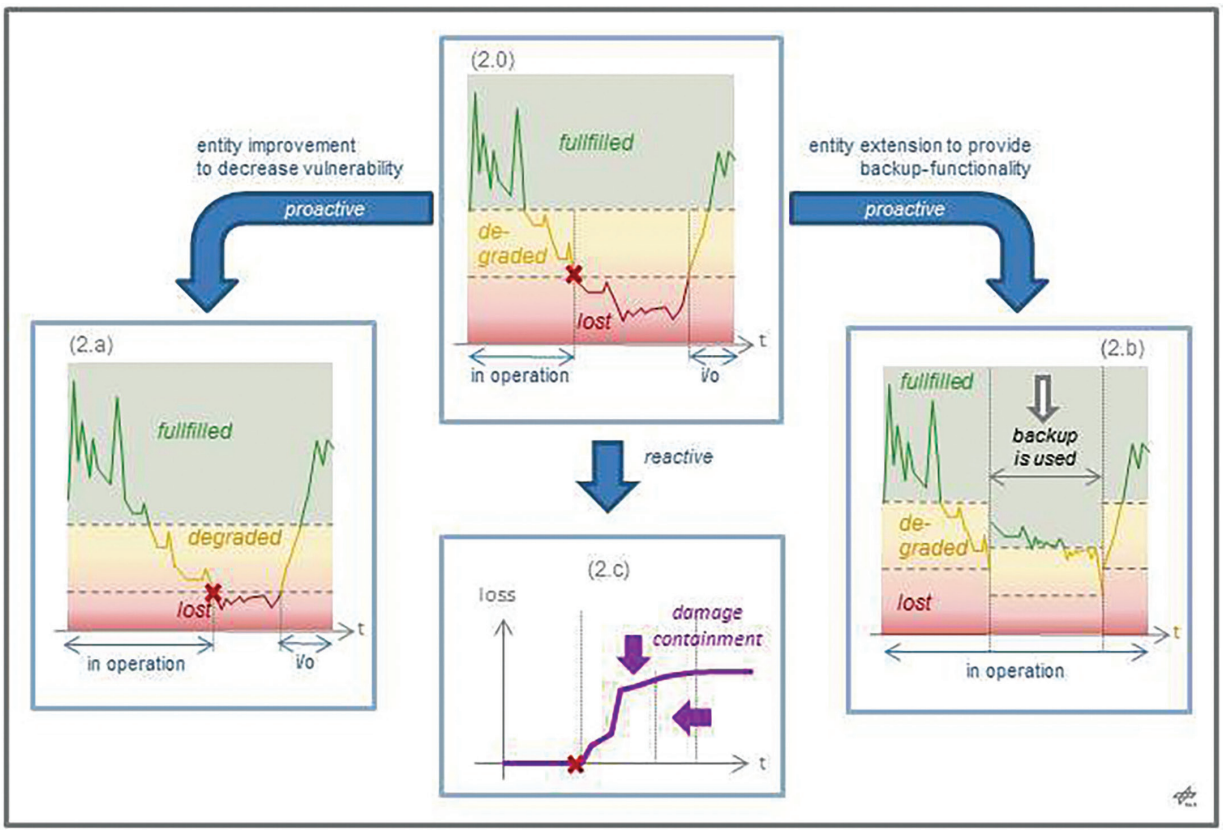

Figure 2 Classical ways to increase the resilience of an entity
Slika 2. Standardni načini povećanja otpornosti subjekta

and finite resources require an integrated view of all entity levels – technological, functional, operational, organisational, administrative, as well as regulative – to find out not only new, but also more effective ways to strengthen resilience.

2. SAFETY, SECURITY AND SAFETY OBJECTIVES / *Sigurnost, zaštita i ciljevi sigurnosti*

Most people associate safety with the absence of unwanted outcomes such as incidents, accidents or unintended events [4]. Therefore, the avoidance of adverse outcomes may be considered as the generalised objective of safety, which should be achieved with the highest probability that is needed and still be acceptable. In a particular case, the fulfilment of safety (as well as the non-fulfilment) depends on the specific objective of safety taking into account causes andeffects (Fig. 3). For example, the objective of occupational safety is the avoidance of working accidents.The operational safety of an entity may be considered as fulfilled, if at least an interruption-free operation is achieved under normal conditions. A higher objective of operational safety includes, in addition to interruption-free operation, the avoidance of work accidents and the protection of the environment. More generally, operational safety of an entity is fulfilled if the operation of the entity itself is the measure of fulfilled operational safety. The growing complexity of entities increases the number and variety of specific targets that must be met to achieve the entity's operational safety. The occurrence of anomalies as well as environmental and climatic changes require a further strengthening of the entity's components and technologies to ensure that operational safety may also be met in the future (Fig. 3: extended operational safety). In times of continuous security threats (e.g. terrorism, criminality, vandalism) the operational safety of an entity increasingly requires the consideration of security-relevant issues. These cover the detection and assessment of threats as well as the establishment of an effective and coordinated safety and security management (Fig. 3: extended operational safety and security).

Independently, if the operational safety of a complex entity or specific safety/security aspect is to be considered, unambiguous measures are needed to formulate and quantify the achieved and target level of safety. Data of accidents and incidents are often collected on behalf of politicians and authorities. Such databases are used to investigate causes of accidents, to evaluate their risk potential, as well as to identify and prioritise the need for further improvements of the entity. For example, the European Maritime Safety Agency (EMSA) is one of the organisations investigating the occurrence and causes of casualties and incidents in the maritime traffic system [1]. EMSA defines a casualty as an event directly connected with the ships' operation and the occurrence of death or injury to persons, loss and destruction of ships and marine infrastructures, stranding and disabling of ships, or pollution of and/or damage to the marine habitat. A study shows that between 2011 and 2014 the number of casualties has more than doubled in Europe [1]. This illustrates the still existing need to continue the enhancement of safety at sea including the maritime infrastructures. Main causes of casualties (~ 60%) are the loss of ship control, collision with floating and fixed objects (without grounding), and collision with other traffic participants [1]. In hindsight, this makes it difficult to reliably reproduce how the causes, effects and events originated and developed, and what their interdependencies were. For example, the loss of navigation control may be caused by a collision with a floating container and could result in a further collision with other traffic participants. Alternatively, equipment failure as well as operator errors may also be accountable for the loss of navigation control and the resulting ship collision. These consideration focus on the identification of possible causes that may result in a loss of safety. Consequently, measures to enhance safety cover either the elimination of possible causes (e.g. increase resilience of the propulsion system against operating errors and destruction) or the establishment of barriers to mitigate their impact (e.g.

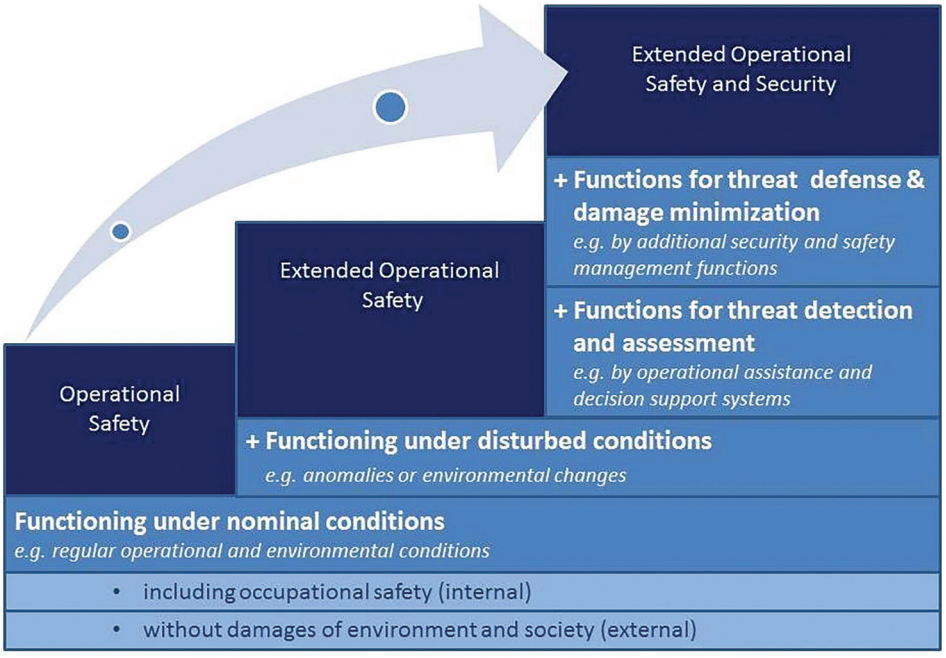

Figure 3 Safety and security aspects
Slika 3. Aspekti sigurnosti i zaštite

training of propulsion operators or implementation of access restrictions).

The increasing complexity of entities makes it increasingly difficult to consider safety based only on simple cause-effect-relationships. The use of new technologies, the scarcity of personnel resources, and changes in organisational structures and responsibilities all add to the emergence of new threats. Additionally, the impact and dynamics of known threats (e.g. climate change, terrorism) are constantly on the rise. Both developments imply that a solely reactive and cause-orientated safety management system is inadequate to maintain or enhance the safety of entities in the future [4]. Going back to the example mentioned above, the probability of colliding with floating containers could be reduced by a global network of container search and recovery services. However, the probability of a collision will never be zero because there will always be a certain time lapse between loss and recovery. But a loss of navigation control should not necessarily result in an accident. Therefore, this safety objective of the 'system ship' (no accident) may be fulfilled even though the safety objective of the 'system propulsion' (interruption-free operation) is not given. With increasingly complex systems in particular, often referred to as 'system of systems', it is neither feasible nor affordable for all components, systems, and players to meet their individual safety objectives. Consequently, entities as well as involved stakeholders should be empowered to continuously monitor internal and external conditions, to predict developments with respect to all event types, and to initiate compensation measures in an effective way, if necessary. In this context, the human is a very important resource to ensure the operational flexibility and resilience of complex entities [4].

As discussed in [4], it is not sufficient to derive an entity's functionality from the performance of its individual systems and components by considering simple cause-effect-relationships. The latter allows only the consideration of cases, where "something goes wrong" results in "unwanted outcomes such as incidents or accidents" [4]. A deeper understanding of the entity is necessary to achieve a state in which the entity is able "to succeed under varying conditions, so that the number of intended and acceptable outcomes is as high as possible" [4]. This also includes those cases, where "best practice" and flexible acting enable that "something goes wrong" will not result in unwanted or disruptive events. Monitoring in real time, performance-driven control, as well as continuous situational assessment are a few new ways to increase the resilience of an entity (see Fig. 4).

The left graph (4.a) illustrates the benefit of integrity monitoring and evaluation. This is a measure to determine the current status, performance and behaviour of safety-critical entities, more or less exactly. For this purpose, a set of observations and performance parameters are monitored, fused and evaluated in real time. In this context alert limits act as decision criteria to differ between fulfilment and non-fulfilment of performance requirements, as well as usability and non-usability of the entity and included components. These assistance functions provide support to operators and users of entities wanting to obtain comprehensive situational pictures, avoid misinterpretations of situational pictures, and consequently prevent the improper use of the entity. The establishment of reliable system awareness by intelligent integrity monitoring and evaluation is therefore important to increase the resilience of safety-critical entities. For example, the relation between ice thickness of an ice field and the ice class of a ship determines whether crossing the ice field is safe or whether it should be circumnavigated. An erroneous estimation of ice thickness may result in economic losses (circumnavigation as a result of a false alarm) or in hazardously misleading operations (crossing the field under increased hazard). As a further example, safe transport of passengers should also include the protection of passengers against criminal and terrorist attacks at crucial points, such as ferry terminals and on board a ferry.The middle graph (4.b) illustrates the case in which continuously monitored performance parameters are used to describe the current situational picture (blue solid line) of the entity and to forecast the behaviour of the entity (blue dotted line). If the degradation/ loss of entity functionality can be forecast, sufficient lead time may be gained to initiate measures improving resilience by early maintenance, timely decommissioning, as well as proactive damage containment. This approach requires an extended entity model, which supports a parametrised description of the situational picture and its changes, including the emergence and avoidance of disruptive events. In addition to the need for

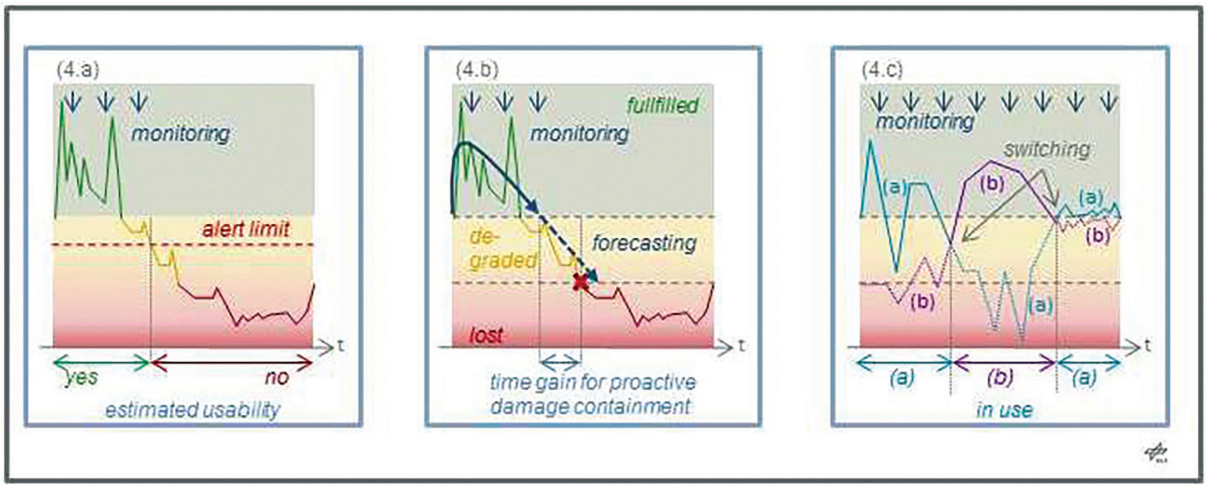

Figure 4 Additional ways to increase the resilience of an entity
Slika 4. Dodatne metode poboljšanja otpornosti subjekta

correct modelling, the effectiveness of this approach hinges on determining the needed parameter with the required accuracy and reliability. For example, by monitoring the wear and tear of parts it is possible to determine the optimal time for procuring spare parts and carrying out maintenance. Likewise, the detection of and defence against terrorist attacks require the screening of traffic situations above and below the sea surface.

A redundancy of architectural and functional levels allows the functionality of an entity to be achieved by alternative independent means (right graph 4.c). This increases the continuity and reliability of the operational level, albeit not perfectly. However, here too, monitoring the systems' performance is an essential prerequisite to achieve an effective switching between alternative options by the entity control. Using Radio Detection and Ranging (RADAR) and Automatic Identification Systems (AIS) as independent and complementary information sources is a well-known approach to improve the surveillance and assessment of maritime traffic situations as a prerequisite for successful collision avoidance. The additional and coordinated use of space-based and airborne monitoring techniques has become necessary to achieve comprehensive situational pictures along coastlines for customs and coast guards. All examples shown in Figure 4 illustrate that the monitoring of the status, performance and behaviour of entities has become more and more important for an effective assessment and management to ensure the entity's resilience in relation to diverse objectives. It also highlights that resilience of complex systems with a wide range of performance and possible emerging threats requires an anticipatory consideration of developments and events, both positively and negatively [3].

3. INDICATORS FOR MONITORING AND CONTROLLING SAFETY AND SECURITY / *Indikatori nadzora i kontrole sigurnosti i zaštite*

Key Performance Indicators (KPIs) are parameters used to specify or indicate the required or achieved capability of an entity. KPIs may beeconomical, ecological, social or technological parameters, which are considered at specific moments or over longer periods of time. They are suitable for describing the behaviour of an entity, to formulate targets or to act as an indicator, in case something goes wrong. For example: the Gross National Product (GNP) is an economic KPI of a society. Turnover and profit of a shipping company are typical business KPIs, which may be correlated to individual business segments (e.g. ship operation, fleet management, and logistic). Associated technological KPIs are related to the operational capability and reliability of systems, services, and components, as well as the means to protect these against any terrorist or criminal attack and other harmful influences. For example, the reliable operation of information technology in all business segments is a safety-relevant KPI; the reliable protection of IT-systems against cyber-attacks is a security-relevant KPI. This illustrates that KPIs, even though used from different perspectives, often depend on each other, and are increasingly affected by safety- and security-relevant issues. Consequently, the resilience of an entity is measured and specified based on its performance and outcomes formulated by KPIs [5]. For example, the Baltic and International Maritime Council (BIMCO) developed a KPI system as standard for the definition, measurement and reporting on the operational performance of ships [7].

In general, a variety of factors determine whether a certain KPI of a complex entity can be met. These factors may be specified by KPIs of the entity's components (system of systems approach). In our example, an optimal functioning of the IT-systems is an essential prerequisite for the turnover and profit of a shipping company. When looking at the individual components, these factors are rather expressed by internal Performance Parameters (iPP) and their associated thresholds (min(iPP),max(iPP)) to describe the nominal behaviour of implemented functions. Coming back to our example, a seamless and safe operation of a ship requires, among other things, the reliable provision of all navigation-relevant information. Therefore, the reliable on-board provision of positional, navigation, and time data (PNT) is one of the associated KPIs on the technological level. For navigation at open sea it is sufficient to know the ship's position with an uncertainty of a few 10 metres. However, during port operation and docking,nautical information (e.g. horizontal or three-dimensional attitude of the ship's hull, electronic nautical charts, geo-referenced port infrastructure and topography) with greater accuracy is needed to avoid collisions. The current application context determines which of the iPPs and thresholds should be fulfilled for seamless and safe ship operation. KPIs as well as iPPs specify either the "As-Is" (status) or the "To-Be" (requirement) of entities taking into account safety as well as security aspects.

Key Risk Identifiers (KRIs) are parameters used to describe and evaluate the risk profile of an entity. KPIs as well as iPPs may serve to determine KRIs, whether they are suitable to detect threats, to estimate the likelihood of occurrence, or to estimate and quantify potential impacts and outcomes. Therefore, KRIs may also be economic, social, business or technological parameters observed over longer periods (to observe trends) or instantaneous parameters (to monitor the current status). At the latest, if a KRI attains unacceptable values, measures may be initiated to retain or recover the entity's functionality or to reduce negative impacts. For this purpose the entity should possess absorptive, adaptive and restorative capabilities to be resilient [3, 5]. At an operational level the initiation, selection, and realisation of absorptive, adaptive and restorative functions are controlled by Key Control Identifiers (KCIs), which are used to formulate decision-making criteria as well as control parameters. However, KCIs may also be used to determine the point in time at which a reengineering of the entity becomes inevitable. If again we consider "Reliable ship operation" as the KPI of interest, then performance degradation and interruptions to the provision of on-board PNT data are typical risk indicators for a possible decrease in the ship's operational safety. Depending on the magnitude and duration of the performance loss, certain KCIs may trigger a switch from automatic to manual operation of navigational tasks. If the frequency of such events becomes unacceptable, a further KCI may initiate an unscheduled maintenance or the reengineering of the on-board PNT system.

4. RESILIENCE ENGINEERING APPROACH / *Pristup temeljen na inženjerstvu otpornosti*

Figure 5 illustrates a way to consider, improve and ensure the resilience of maritime infrastructures based on a system-of-systems approach in a multi or N-dimensional manner respectively. The light-blue box represents the considered entity, e.g. a port, during its continuous lifecycle. Most

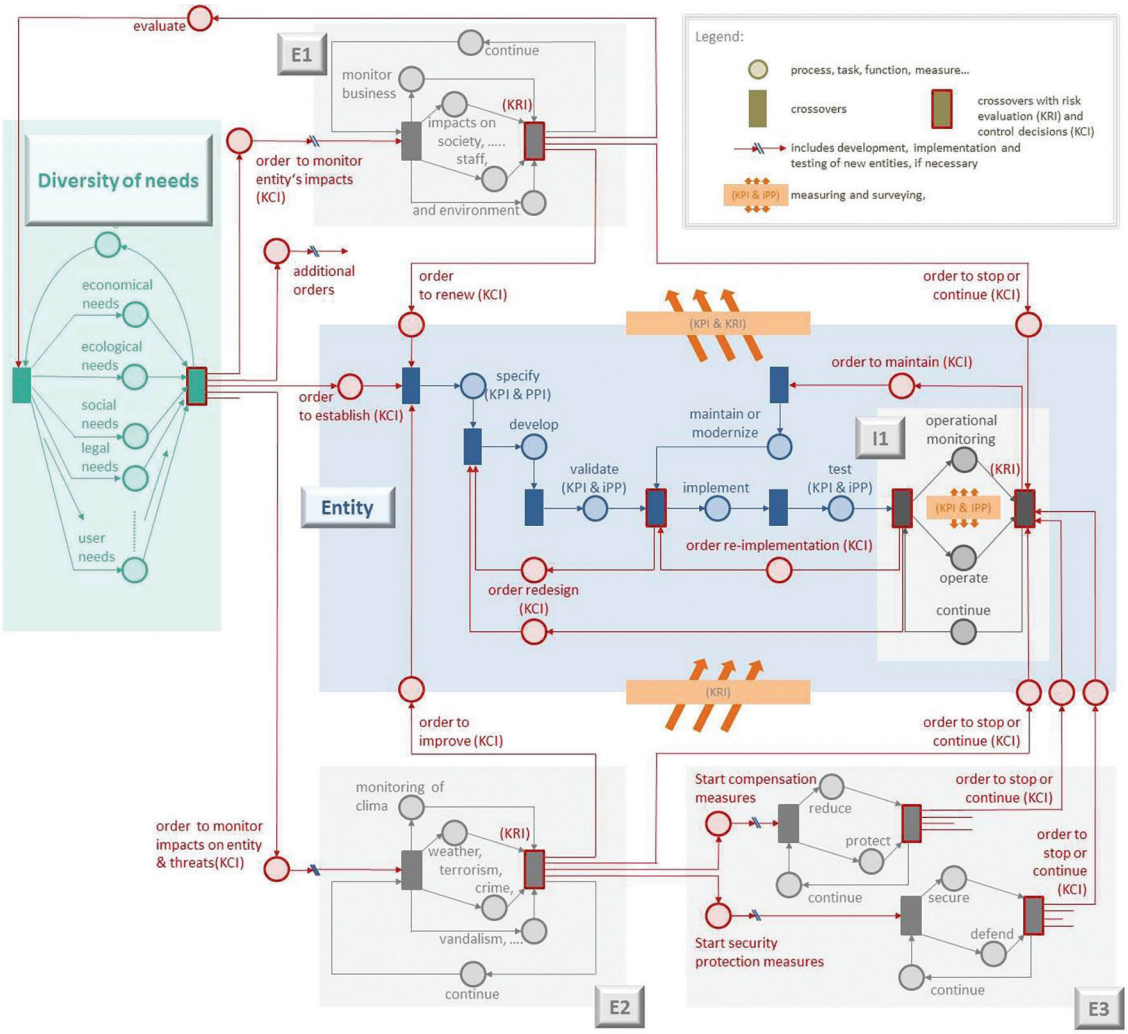

Figure 5 Resilience^{N} approach: Comprehensive views on proactive and reactive aspects of resilience engineering
Slika 5. Pristup temeljen na otpornosti: Sveobuhvatni pogled na proaktivne i reaktivne aspekte inženjerstva otpornosti

major ports today arose many centuries ago to facilitate the shipborne trade. Since then social, economic and ecological evolution, as well as changes in user needs, have resulted in the continuous development and extension of global port infrastructures (modelled by the light-green box). For example, the establishment of new and greater container terminals in the last decades is a result of the continually increasing demand for higher transport capacity and efficiency. If the discrepancy between achieved and target performance of an entity becomes intolerable, the 'order' to establish a further entity is triggered (e.g. offshore port).

The establishment of an entity is based on a sequence of processes: specification of KPIs and iPPs, development, validation, implementation and testing (dark-blue processes), whereby validation and testing serves as quality assurance during the establishment process. A failed test indicates that KCIs have initiated either the re-implementation or the redesign of an entity. On the other hand, if the established entity is able to meet the operational performance formulated by KPIs and iPPs under nominal operational conditions, the test is passed. This covers the fulfilment of operational safety as well as the achievement of operational targets and the avoidance of negative impact on business, staff and environment. An effective mix of internal and external monitoring processes (within box I1 and provided by E1) assesses the entity's behaviour, performance and status. If any endangerment is identified (KRI's), the derived KCIs start the maintenance or modernisation of the entity. However, the monitoring of entities in the global context (E1) may also result in new insights, which will reshape the different needs in relation to the entities and their operation. For example, the provision of power supply systems at terminals is a measure of port modernisation that reduces the exhaust emission of cruise liners and other vessels during their berthing times. The frequency of rapidly changing threats increases and is often induced by climatic changes, extreme weather conditions, or growing vandalism, crime and terrorism. The monitoring of these threats (E2) helps to evaluate whether a redesign is necessary to increase the resilience of the entity. The aim of the redesign is the improvement of the entity to meet iPPs and KPIs for a larger range of operational conditions. The monitoring of a threat situation in real time enables to initiate compensation and security protection measures (E3) as far as possible, if necessary. Such measures in the case of a port may be that port authorities deny ships to enter or leave the port during extreme autumn storms. An early identification of leakages at LNG terminals makes it possible for the disaster management to save lives and goods in the port area by fast evacuation of hazard-prone areas. If surveillance systems are operated, unauthorised movements

and safety-critical events may be detected in the port area. This helps to avoid any attacks on port infrastructure and operation. In extreme cases, where safety and security cannot be ensured despite applied resilience measures, the entity should be taken out of operation temporarily or permanently.

The integrated presentation of different processes in Figure 5 may suggest that resilience is considered to be a technological challenge in this article. It should be noted that the specification of key risk indicators and resulting key control indicators is generally the task of humans giving due consideration to all interests and priorities. However, in these times of digitalisation and automation, decision processes may also be carried out by machines and processes that are conditioned to a certain level of artificial intelligence.

5. CONCLUSION / *Zaključak*

On a general level, this article addresses the question of which proactive and reactive aspects should be considered to achieve a resilient entity. First, classical and new ways to increase the resilience of an entity were presented followed by the definition of indicators that can be used to monitor and control the safety and security on a system-of-systems level. Finally, the so-called resilience^{N} approach was presented in order to define a model-based comprehensive view on proactive and reactive aspects of resilience engineering, covering not only internal but also external factors. Our intention is to use this toolkit for the development and optimizationof resilience concepts for different safety-critical maritime infrastructures. As shown, it is important to specify and evaluate the level of an entity's resilience using KPIs, iPPs, and KRIs in real time as well as for longer periods of time. Our next step towards comprehensive situational surveying of entities is the development of status models needs to be pursued to enable the monitoring of emerging risks and for early initiation of compensation and defence measures, if necessary.

REFERENCES / *Literatura*

[1] EMSA: Annual overview of marine casualties and incidents (2015). Available from https://www.cesam.org/documents/Review_Marine_Casualties_and_Incidents_2015.pdf

[2] European Commission: The EU approach to resilience: learning from food security crises, communication from the commission to the european parliament and the council, COM (2012) 586 final, Brussels, 3.10.2012,available from http://ec.europa.eu/echo/files/policies/resilience/com_2012_586_resilience_en.pdf

[3] Fiksel, J.: Designing resilient, sustanable systems. Environ. Sci. Technol. 2003 (37), page 5330-5339, available fromhttp://www.ce.cmu.edu/~gdrg/readings/2007/01/16/Fiksel_DesigningResilientSustainableSystems.pdf

[4] Hollnagel, E. & Leonhardt, J. & Licu T. & Shorrock, S. (2013) From Safety-I to Safety-II, A White Paper. Published by European Organisation for the Safety of Air Navigation (EUROCONTROL). Available from http://www.skybrary.aero/bookshelf/books/2437.pdf

[5] Sansavini, G. (2016) Engineering Resilience in Critical Infrastructures. Proceedings of the NATO Advanced Research Workshop on Resilience-based Approaches to Critical Infrastructures Safeguarding. Azores (Portugal). 26-29 June. Springer (DOI 10.1007/978-94-024-1123-2, page 189-203. https://doi.org/10.1007/978-94-024-1123-2

[6] United Nations Office for Disaster Risk Reduction (UNISDR): UNISDR terminology on disaster risk reduction. (2009) Genueva, available from http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf

[7] BIMCO: The Shipping KPI Standard V2.6, Released 09 January (2017). Available from https://www.shipping-kpi.org.

[8] Schröder-Hinrichs, J.-U., Prätorius, G., Graziano, A., Kataria, A., & Baldauf, M. (2015):Introducing the Concept of Resilience into Maritime Safety, Paper presented at the 6th REA Symposium, Lisbon, Portugal.